REMARKS

Claims 1-21 are pending. Claim 1 is the only independent claim. Favorable reconsideration is respectfully requested.

Claims 1-16 and 19-21 were rejected under 35 U.S.C. § 103 over U.S. Patent 7,350,076 (Young et al.) in view of U.S. Patent Publication 2004/0103283 (Hornak). Claims 17 and 18 were rejected under 5 U.S.C. § 103 over Young et al. and Hornak, and further in view of U.S. Patent 5,515,439 (Bantz et al.). Applicants submit that independent claim 1 is patentable over the cited art for at least the following reasons.

The Office Action conceded that Young failed to disclose the feature "wherein when a mobile terminal (MT) logs on a wireless Access Point (AP), a Mobile Terminal (MT) certificate and an Access Point (AP) certificate are transferred to an Authentication server (AS)....in order to achieve the direct two-way certificate authentication between said Mobile Terminal (MT) and Access Point (AP)" of claim 1. However, the position was taken that such features are taught by Hornak. Applicants disagree.

The authentication process of Hornak can be divided into two phases, with the first phase relating to authentication during the certificate issuance process and the second phase relating to authentication when the communication entities use the certificates. In the first phase, the trusted third party CA is responsible for certificate issuance to the three entities such as Client, Gateway and Origin Server respectively (see, e.g., Hornak, paragraphs 0014 and 0084). Authentication in this phase will guarantee that the certificates obtained by the three entities are authenticated and signed by the Certification Authority CA. Paragraph 0083 of Hornak, identified by the examiner, describes the authentication process in this first phase.

During the second phase, the Client communicates with the Gateway under a certain protocol to exchange certificates with each other. Each party authenticates the formality correctness of the other's certificate according to the public key (CA-PK) of CA included thereof and obtains the public key information of the other party. In particular, the Gateway obtains the public key of the client (C-PK) and the Client obtains the public key of the Gateway (G-PK). Thereby the two

way authentication is achieved. Depending on the other party's public key information, the two parties negotiate the master key for communication and start private communication using WTLS. (See, e.g., Hornak, paragraph 0013; paragraph 110). Similar protocol exchange as that between the Client and the Gateway is made between the Gateway and the Original Server and private communication using SSL or TLS begins after the master key is negotiated. (See, e.g., Hornak, paragraphs 111-114). Therefore, according to Hornak, during the second phase when certificates are in use, certificates authentication is accomplished by exchanging certificates between the two communication entities. (See, e.g., Hornak, lines 12-15 of paragraph 0014; lines 1-5 of paragraph 0021).

According to the solution of Hornak, by authentication in the certificate issuance process (corresponding to the first phase), any user can authenticate weather the certificate is issued by the alleged issuer based on the information of the issuer (normally means the public key information of the issuer). However, in practice, the public key certificate owned by a device as its unique identifier can be revoked or becomes invalid due to divulgence of the private key or other reasons. If the invoked or invalidated certificates are still in use, secure communication between two parties can not be guaranteed. Unfortunately, the solution of Hornak cannot address this problem since it presumes any certificate in use is valid as far as it has been authenticated in the issuance phase. In Hornak, during the second stage, authentication is achieved simply by exchanging the certificates between the two entities.

Claim 1 solves this problem and achieves real-time authentication of the certificates not only regarding formality, but also validity when they are in use. Compared with Hornak the invention of claim 1 focuses on the second phase authentication and takes a different authentication solution in this phase. In particular, claim 1 makes use of the trusted third party---Authentication Server -- to authenticate the status of the certificates in order to achieve real-time and flexible management of the devices. According to the technical feature "the Mobile Terminal (MT) certificate and the Access Point (AP) certificate are transmitted to the Authentication Server (AS) and are authenticated through the Authentication Server (AS)" in claim 1, the Authentication Server authenticates not only the formality but also the status validity of the certificates. Therefore, it can

make real-time judgment about whether the identities of the mobile terminal MT and the wireless access point AP are legal.

The authentication of the certificates by the Authentication Server of the claimed invention is not equivalent to the formality authentication of the certificates exchanged between the Gateway and Client by authenticating the signature portions of the other party defined in Hornak. Although it might seem in Hornak the two parties also perform two way certificate authentication, in fact only the formality of the other party's certificate is authenticated by each party, instead of the legal status of the certificates. Therefore, the object of authentication has not been achieved. Consequently, it cannot be guaranteed that the legal user is using the legal network.

With reference to Fig. 5 of Hornak and the corresponding description, it will be easy for the person skilled in the art to understand that what is described in paragraph 0083 (on page 5): "[T]he CA 48 is accessible by the client 42, the origin server 44 and the gateway 46 for authentication of a certificate belonging to each of these parties" is different from the definition "when a Mobile Terminal (MT) logs on a wireless Access Point (AP), the Mobile Terminal (MT) certificate and the Access Point (AP) certificate are transmitted to the Authentication Server (AS) and are authenticated through the Authentication Server (AS)" of claim 1.

In Hornak, during the certificate issuance stage (first phase), CA issues signed certificates to the three entities Client, Gateway and Original Server. However, in the claimed invention, AS authenticates the certificates of the MT and AP "when Mobile Terminal (MT) logs on wireless Access Point (AP)" (claim1).

Furthermore, the description of Hornak's paragraph 110 (on page 6): "a protocol handshake is executed between the client 42 and the gateway 46" is different from what is defined in claim 1: "then the authentication result of the Mobile Terminal (MT) certificate and the Access Point (AP) certificate is returned to the Access Point (AP) and the Mobile Terminal (MT) in order to achieve the direct two-way certificate authentication between said Mobile Terminal (MT) and Access Point (AP)". It can be seen, in Hornak, that when the certificates are in use (second phase), certificates exchange, formality authentication of the certificates and negotiation of the communication master key are all performed between the two entities Client and the Gateway and

do not involve the CA. While in the claimed invention, with three entities involved at this stage, AS returns the authentication results to the Access Point and the Mobile Terminal. Thereby mutual authentication between MT and AP are achieved by the involvement of AS.

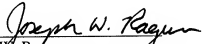
In summary, applicants submit that Hornak fails to disclose or suggest the technical features of the claimed invention as alleged in the Office Action.

For at least the foregoing reasons, claim 1 is believed clearly patentable over Young et al. and Hornak. The dependent claims are believed patentable for at least the same reasons as claim 1. The other references are not believed to remedy the abovementioned deficiencies of the cite art.

In view of the above remarks, applicants believe the pending application is in condition for allowance.

Dated: June 22, 2010

Respectfully submitted,

By 

Joseph W. Ragusa
Registration No.: 38,586
DICKSTEIN SHAPIRO LLP
1633 Broadway
New York, New York 10019-6708
(212) 277-6500
Attorney for Applicant